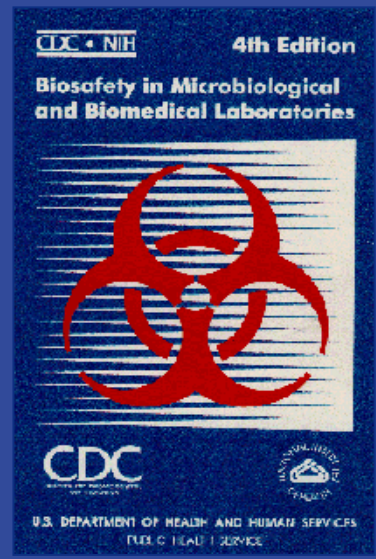
Security of Select Agents at Bioscience Facilities

Reynolds M. Salerno, Ph.D.
Sandia National Laboratories
US Department of Energy

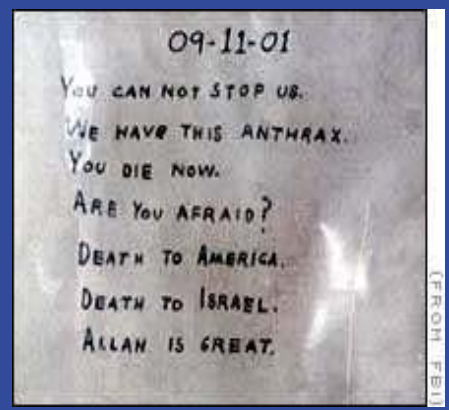
Biosafety vs. Biosecurity

- Biosafety
  - Objective: reduce or eliminate accidental exposure to or release of potentially hazardous agents
  - Strategy: implement various degrees of laboratory "containment" or safe methods of managing infectious materials in a laboratory setting
- Biosecurity
  - Objective: protect against theft or diversion of select agents
  - Strategies
    - Define risk by evaluating probabilities and consequences
    - Protect defined assets against defined threats
    - Apply a graded protection approach
    - Integrate security technologies and procedures
    - Impact operations only to the level required



Need to Secure Select Agents

- Aim of biosecurity is to mitigate BW threat at the source
  - Prevent terrorists or proliferant states from acquiring select agents from government, commercial, or academic facilities
- Securing select agents is an important element of comprehensive BW nonproliferation programs
  - Cannot prevent BW terrorism or proliferation
  - Must be augmented by other national mechanisms



Challenges to Securing Select Agents

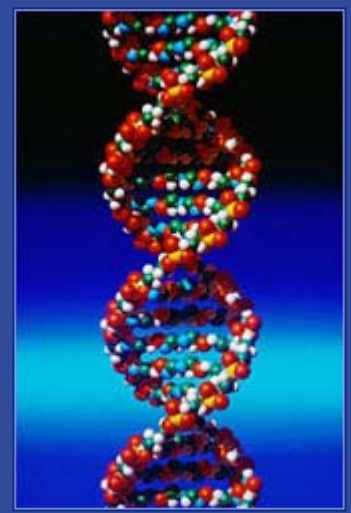
- Dual-use characteristics
  - Valuable for many legitimate, defensive, and peaceful commercial, medical, and research applications
- Nature of the material
  - Living and self-replicating organisms
  - Used in very small quantities
  - Cannot be reliably quantified
  - Exist in many different process streams in facilities
  - Contained biological samples are virtually undetectable
- Laboratory culture
  - Biological research communities not accustomed to operating in a security conscious environment

Biosecurity Cost Benefit Considerations

- Bioscience facilities are not unique repositories
  - Most agents can be isolated from nature
  - Many similar collections of agents exist worldwide
- Relatively few agents can be easily grown, processed, weaponized, and successfully deployed while maintaining virulence/toxicity
  - Very few agents used as a weapon could cause mass human, animal, or plant casualties
  - Not all agents equally attractive to adversaries
- Need a methodology to make informed decisions about how to design an effective and efficient biosecurity system

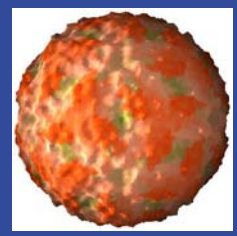
Biosecurity Methodology

- Qualitative risk and threat assessment is the essential first step
  - Process should include scientists, technicians, managers, security professionals, and law enforcement (counter-terrorism) experts
- Asset identification and prioritization
  - Consequences of diversion and adversary attractiveness
- Threat identification and prioritization
  - How would an adversary steal the defined assets?
- Risk and threat assessments establish design parameters and protection principles



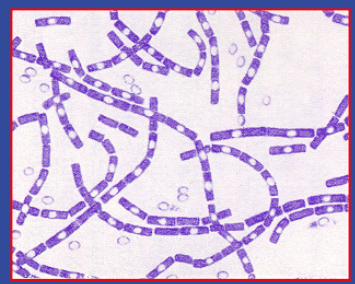
Asset Identification and Prioritization

- Primary consequence
  - Loss could lead to national security event (bioterrorism)
  - Certain biological agents
- Secondary consequence
  - Loss could assist in achieving a primary consequence or access to a primary asset
  - Certain information related to select agents
- Tertiary consequence
  - Loss could affect operations
  - Certain facilities, equipment, etc.



FMD virus

Yersinia pestis



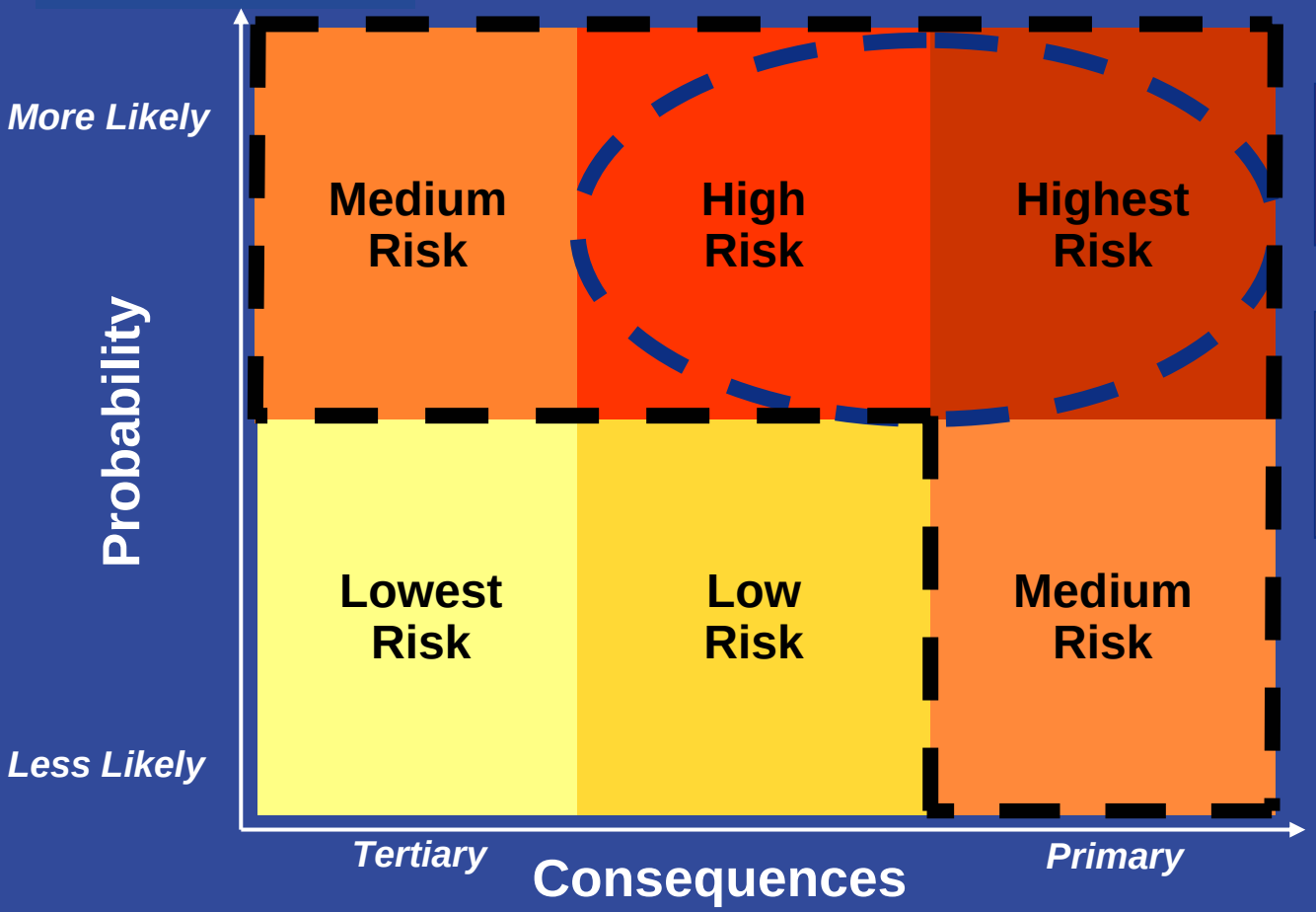
Bacillus anthracis

Fermentation vessel

Threat Identification

- Adversary categories
  - Insider with authorized access
  - Invited outsider(s) – visitor
  - Outsider(s) with limited access and system knowledge
  - Outsider(s) with no access and general knowledge
  - Collusion between an insider and an outsider
- What will the adversaries aim to do?
  - Steal agents, steal information, disperse agents, destroy/deface facility, steal equipment, etc.
- How will the adversaries perpetrate the event?
  - Alone or in a group? Armed or unarmed? Covert or overt?

Risk Prioritization



- **Protect against high risk scenarios**
- **Develop incident response plans for medium and low risk scenarios**

Generic Biosecurity Design Parameters

- Highest risk scenarios
  - Insider, visitor, or outsider with limited access attempting to steal select agents covertly
- High risk scenarios
  - Insider, visitor, or outsider with limited access attempting to steal select agent-related information covertly
- Medium risk scenarios
  - Small outsider groups that would aim to destroy or deface the facility
- Terrorist commando assault unlikely
  - Agents available elsewhere
  - Overt attack using force would signal authorities to take medical countermeasures

Generic Biosecurity Protection Principles

- Personnel Reliability
- Physical Security
- Information Technology Security
- Material Control and Accountability
- Material Transfer Security
- Program Management

Typically excludes substantial perimeter systems and armed guard forces

Personnel Reliability

- Allow access only to those individuals who have
  - Legitimate need to handle select agents
  - Appropriate training in biosafety, containment, and security procedures
- Conduct background investigations on employees
- Establish visitor interaction procedures
  - Screening, badging, and escorting
- Report suspicious activity

Physical Security

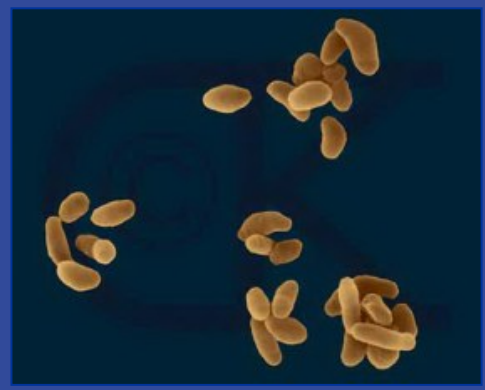
- Implement systems to deter, detect, and respond to unauthorized attempts to gain access to select agents
- Establish graded protection areas with
  - Intrusion detection
  - Access controls and transaction recording
  - Alarm assessment capabilities
  - Physical barriers and delay systems
  - Law enforcement response capabilities

Material Control and Accountability

- Develop systems to document
  - What materials exist in a certain facility
  - Where they are located
  - Who is responsible for them
  - Who has access to them
- Avoid trying to apply quantitative material-balance inventory accounting principles

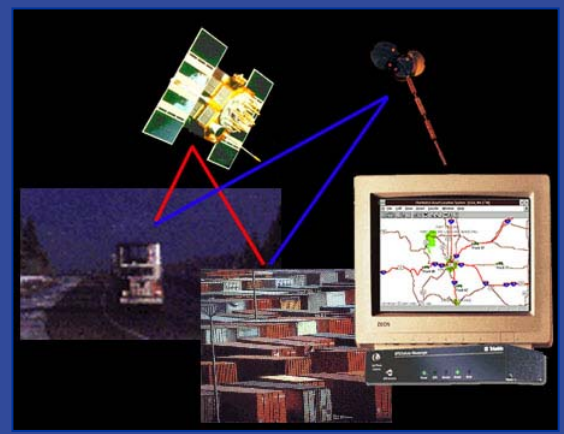
Material Transfer Security

- Document, account for, and control select agents when they are moving between protected areas within a facility
- Receive authorization and monitor external transfers between registered facilities before, during, and after transport



Information Technology Security

- Control access to sensitive information related to select agents
- Establish policies and implement technologies for handling, using, and storing paper-based, telephonic, photographic, and electronic media



Program Management

- Provide policy oversight and implementation of the biosecurity program
- Maintain documentation of
  - Security plan
  - Incident response plan
  - Security training program
  - Self-assessment and auditing program

Summary

- Necessary to take steps to reduce the likelihood that select agents could be stolen from bioscience facilities
- Critical that these steps are designed specifically for biological materials and research so that the resulting system will balance science and security concerns